

AMENDED IN SENATE MAY 23, 2005
AMENDED IN SENATE MAY 10, 2005
AMENDED IN SENATE APRIL 26, 2005
AMENDED IN SENATE APRIL 18, 2005
AMENDED IN SENATE APRIL 13, 2005

SENATE BILL

No. 852

**Introduced by Senator Bowen
(Coauthor: Senator Alquist)**

February 22, 2005

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to identity theft.

LEGISLATIVE COUNSEL'S DIGEST

SB 852, as amended, Bowen. Identity theft.

Existing law requires any agency, or a person or business conducting business in California, which owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law allows that notification to be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

This bill would require an agency, or a person or business conducting business in California, that owns, licenses, or collects computerized data that includes the personal information of a California resident, to notify the resident of any breach of the security of the data, as specified, regardless of whether the data was

computerized when it was acquired. The bill would also revise the definition of personal information in this context and would prescribe that a request by a law enforcement agency to delay notification be in writing *or made electronically*, as specified.

By adding to the duties of local law enforcement agencies, this bill would impose a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that, if the Commission on State Mandates determines that the bill contains costs mandated by the state, reimbursement for those costs shall be made pursuant to these statutory provisions.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: yes.

The people of the State of California do enact as follows:

- 1 SECTION 1. Section 1798.29 of the Civil Code, as added by
- 2 Section 2 of Chapter 1054 of the Statutes of 2002, is amended to
- 3 read:
- 4 1798.29. (a) Any agency that owns, licenses, or collects
- 5 computerized data that includes personal information shall
- 6 disclose any breach of the security of the system following
- 7 discovery of the breach in the security of the data, or upon receipt
- 8 of notice under subdivision (b), to any resident of California
- 9 whose personal information was, or is reasonably believed to
- 10 have been, acquired by an unauthorized person, regardless of
- 11 whether the data was in computerized form at the time of the
- 12 unauthorized acquisition. The disclosure shall be made in the
- 13 most expedient time possible and without unreasonable delay,
- 14 consistent with the legitimate needs of law enforcement, as
- 15 provided in subdivision (c), or any measures necessary to
- 16 determine the scope of the breach and restore the reasonable
- 17 integrity of the data system.
- 18 (b) Any agency in possession of computerized data that
- 19 includes personal information that the agency does not own shall
- 20 notify the owner or licensee of the information of any breach of
- 21 the security of the data immediately following discovery, if the

1 personal information was, or is reasonably believed to have been,
2 acquired by an unauthorized person, regardless of whether the
3 data was in computerized form at the time of the unauthorized
4 acquisition.

5 (c) If a law enforcement agency determines that the
6 notification will impede a criminal investigation, the notification
7 required by this section may be delayed upon the written *or*
8 *electronic* request of the law enforcement agency. The
9 notification required by this section shall be made without
10 unreasonable delay after the law enforcement agency determines
11 that the notice will not compromise the investigation and so
12 notifies the agency in writing *or electronically*.

13 (d) For purposes of this section, “breach of the security of the
14 system” means unauthorized acquisition of computerized data
15 that compromises the security, confidentiality, or integrity of
16 personal information maintained by the agency, regardless of
17 whether the data was in computerized form at the time of
18 acquisition. Good faith acquisition of personal information by an
19 employee or agent of the agency for the purposes of the agency is
20 not a breach of the security of the system, provided that the
21 personal information is not used or subject to further
22 unauthorized disclosure. The mailing of materials containing an
23 individual’s personal information to the individual’s current
24 postal address or electronic mail address, as reflected in the
25 agency’s records, by an employee or agent of the agency, is not a
26 breach of the security of the system.

27 (e) (1) For purposes of this section, “personal information”
28 means an individual’s last name in combination with any one or
29 more of the following data elements, except as provided in
30 paragraph (2):

31 (A) Social security number.

32 (B) Driver’s license number or California identification card
33 number.

34 (C) Account number or credit or debit card number; or, if a
35 security code, access code, or password is required for access to
36 an individual’s financial account, the account number or credit or
37 debit card number in combination with the required code or
38 password.

39 (2) A name in combination with a data element is not personal
40 information, as specified in paragraph (1), if either the name or

1 data element is encrypted or redacted. However, this exception
2 shall not apply in either of the following cases:

3 (A) Encrypted information was, or is reasonably believed to
4 have been, acquired by an unauthorized person or persons who
5 had access to a key that could be used to decrypt the information.

6 (B) An unencrypted or unredacted data element was, or is
7 reasonably believed to have been, acquired in combination with
8 the individual's address or telephone number.

9 (f) For purposes of this section, "notice" may be provided by
10 one of the following methods:

11 (1) Written notice.

12 (2) Electronic notice, if the notice provided is consistent with
13 the provisions regarding electronic records and signatures set
14 forth in Section 7001 of Title 15 of the United States Code.

15 (3) Substitute notice, if the agency demonstrates that the cost
16 of providing notice would exceed two hundred fifty thousand
17 dollars (\$250,000), or that the affected class of subject persons to
18 be notified exceeds 500,000, or the agency does not have
19 sufficient contact information. Substitute notice shall consist of
20 all of the following:

21 (A) E-mail notice when the agency has an e-mail address for
22 the subject persons.

23 (B) Conspicuous posting of the notice on the agency's Web
24 site page, if the agency maintains one.

25 (C) Notification to major statewide media.

26 (g) Notwithstanding subdivision (f), an agency that maintains
27 its own notification procedures as part of an information security
28 policy for the treatment of personal information and is otherwise
29 consistent with the timing requirements of this part shall be
30 deemed to be in compliance with the notification requirements of
31 this section if it notifies subject persons in accordance with its
32 policies in the event of a breach of security of the system.

33 (h) Regardless of the method by which notice is provided, that
34 notice shall include a description of the elements of personal
35 information that were, or are reasonably believed to have been,
36 acquired by an unauthorized person.

37 (i) A California resident may be determined to be an
38 individual whose current postal mailing address, as reflected in
39 the records of the agency, is in California.

(j) In the event that more than 5,000 California residents are to be notified at one time, the agency shall also notify, without delaying the notice to California residents for this reason, the three consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Sec. 1681a, or their successors, of the timing, content, and distribution of the notices and approximate number of affected persons.

SEC. 2. Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 1054 of the Statutes of 2002, is amended to read:

1798.82. (a) Any person or business that conducts business in California, and that owns, licenses, or collects computerized data that includes personal information, shall disclose any breach of the security of the system following discovery of the breach in the security of the data, or upon receipt of notice under subdivision (b), to any resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person, regardless of whether the data was in computerized form at the time of the unauthorized acquisition. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business in possession of computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person, regardless of whether the data was in computerized form at the time of the unauthorized acquisition.

(c) If a law enforcement agency determines that the notification will impede a criminal investigation, the notification required by this section may be delayed upon the written *or electronic* request of the law enforcement agency. The notification required by this section shall be made without unreasonable delay after the law enforcement agency determines that the notice will not compromise the investigation and so

1 notifies the person or business in writing *or electronically*.
2 *However, a request or notice by a law enforcement agency to a*
3 *person or business pursuant to this subdivision may only be*
4 *made electronically if the person or business is able to receive*
5 *the request or notice electronically.*

6 (d) For purposes of this section, “breach of the security of the
7 system” means unauthorized acquisition of computerized data
8 that compromises the security, confidentiality, or integrity of
9 personal information maintained by the person or business,
10 regardless of whether the data was in computerized form at the
11 time of acquisition. Good faith acquisition of personal
12 information by an employee or agent of the person or business
13 for the purposes of the person or business is not a breach of the
14 security of the system, provided that the personal information is
15 not used or subject to further unauthorized disclosure. The
16 mailing of materials containing an individual’s personal
17 information to the individual’s current postal address or
18 electronic mail address, as reflected in the records of the person
19 or business, by the person or business, is not a breach of the
20 security of the system.

21 (e) (1) For purposes of this section, “personal information”
22 means an individual’s last name in combination with any one or
23 more of the following data elements, except as specified in
24 paragraph (2):

25 (A) Social security number.

26 (B) Driver’s license number or California identification card
27 number.

28 (C) Account number or credit or debit card number; or, if a
29 security code, access code, or password is required for access to
30 an individual’s financial account, the account number or credit or
31 debit card number in combination with the required code or
32 password.

33 (2) A name in combination with a data element is not personal
34 information, as specified in paragraph (1), if either the name or
35 data element is encrypted or redacted. However, this exception
36 shall not apply in either of the following cases:

37 (A) Encrypted information was, or is reasonably believed to
38 have been, acquired by an unauthorized person or persons who
39 had access to a key that could be used to decrypt the information.

1 (B) An unencrypted or unredacted data element was, or is
2 reasonably believed to have been, acquired in combination with
3 the individual's address or telephone number.

4 (f) For purposes of this section, "notice" may be provided by
5 one of the following methods:

6 (1) Written notice.

7 (2) Electronic notice, if the notice provided is consistent with
8 the provisions regarding electronic records and signatures set
9 forth in Section 7001 of Title 15 of the United States Code.

10 (3) Substitute notice, if the person or business demonstrates
11 that the cost of providing notice would exceed two hundred fifty
12 thousand dollars (\$250,000), or that the affected class of subject
13 persons to be notified exceeds 500,000, or the person or business
14 does not have sufficient contact information. Substitute notice
15 shall consist of all of the following:

16 (A) E-mail notice when the person or business has an e-mail
17 address for the subject persons.

18 (B) Conspicuous posting of the notice on the Web site page of
19 the person or business, if the person or business maintains one.

20 (C) Notification to major statewide media.

21 (g) Notwithstanding subdivision (f), a person or business that
22 maintains its own notification procedures as part of an
23 information security policy for the treatment of personal
24 information and is otherwise consistent with the timing
25 requirements of this part, shall be deemed to be in compliance
26 with the notification requirements of this section if the person or
27 business notifies subject persons in accordance with its policies
28 in the event of a breach of security of the system.

29 (h) Regardless of the method by which notice is provided, that
30 notice shall include a description of the elements of personal
31 information that were, or are reasonably believed to have been,
32 acquired by an unauthorized person.

33 (i) A California resident may be determined to be an
34 individual whose current postal mailing address, as reflected in
35 the records of the person or business, is in California.

36 (j) In the event that more than 5,000 California residents are to
37 be notified at one time, the person or business shall also notify,
38 without delaying the notice to California residents for this reason,
39 the three consumer reporting agencies that compile and maintain
40 files on consumers on a nationwide basis, as defined by 15

1 U.S.C. Sec. 1681a, or their successors, of the timing, content, and
2 distribution of the notices and approximate number of affected
3 persons.

4 SEC. 3. If the Commission on State Mandates determines that
5 this act contains costs mandated by the state, reimbursement to
6 local agencies and school districts for those costs shall be made
7 pursuant to Part 7 (commencing with Section 17500) of Division
8 4 of Title 2 of the Government Code.

O